BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

学術刊行物 情処研報 Vol.99, No.11
ISSN 0919-6072

情報処理学会研究報告

99 － EIP － 3

1999年1月30日

社団法人 情報処理学会

目　　次

電子化知的財産・社会基盤　3－3
（99．1．30）

ネットワーク上での情報統合に対するプライバシー保護システムのあり方

橋本 誠志　　金田 重郎

同志社大学大学院総合政策科学研究科

br0111@mail3.doshisha.ac.jp, skaneda@mail.doshisha.ac.jp

あらまし

ネットワーク上に溢れている個人データは，デジタル化されているが故に，統合され，個人のプライバシーが侵害される恐れがある．情報統合を視野に置くプライバシー保護法制は，欧米には存在する．EU 指令は，情報の結合に言及している．また，ドイツ身分証明書法は，個人 ID による情報統合を禁止している．民間部門に対するプライバシー保護法制自体が存在しない我が国と比較すれば，このような法律があるだけでも，西欧諸国の状況は大きく異なっている．但し，ここで想定されているのは，特定属性（キー属性）による統合であろう．キー属性でなくても，複数属性を併用すれば，結果として，キー属性として利用できることにも注意が必要である．いずれにせよ，情報統合によるプライバシー侵害は，データ主体・データ管理者の予知範囲を超えて侵害が発生する．情報統合によるプライバシー侵害は，個々のデータ管理者の善良なる管理監督のみでは防ぎ得ない．我が国でも，情報統合を前提とする法制度の確立と，併せて，データ主体が個人情報の存在を常に把握し得る，個人データ流通管理システム/データ監察官の設置が必要と思われる．

Privacy Protection Systems for Infringement by Combination of Personal Data in a Network

Satoshi HASHIMOTO and Shigeo KANEDA

Doshisha University, Graduate School of Policy and Management

br0111@mail3.doshisha.ac.jp, skaneda@mail.doshisha.ac.jp

Abstract

In this paper the authors discuss a new type of privacy infringement by combination of private information distributed in a computer network. Today many personal data are in it and they are digital data because of our lively social activities and rapid progress of information technology. So everyone can easily unite such data and get complete private information of the person. This situation is in danger of more serious privacy infringement. In Japan in spite of this environment people are little able to know the present condition and whereabouts of their data in the network, having no comprehensive privacy protection law system which supposes privacy infringement by unification of private information such as EU ,Germany ,and etc. Moreover this type of privacy infringement can occur beyond extent which administrator and data subject are to foresee. That is the most important issue of this new type of privacy infringement. This paper demonstrates a concrete example and examines counterplans to solve this problem.

1 はじめに

ネットワーク上のデータは,デジタル化されている故に,複数の情報ソースからの個人データが統合され,個人（データ主体）の全体像が把握される危険を持っている.著者らは既に,ホームページの個人データを氏名により統合できることを論じた [7, 8].

但し,民間部門を対象とするプライバシー保護法が無い我が国とは異なり,欧米には,情報統合を視野に置いたプライバシー保護法システムが存在する.EU 指令は,その条文で情報の結合に言及している.また,ドイツでは身分証明書法の中で個人 ID による統合を禁止している.但し,これら法制では,キー属性による統合（JOIN）を想定している.複数の属性を併用すれば,キー属性として作用する事に注意すべきである.

情報統合では,データ管理者がプライバシーに配慮しても,思わぬ侵害が発生する.特に,プライバシー保護法の無い我が国では,いわゆる名簿屋等の個人情報販売業者により,深刻な問題を引き起こす恐れが強い.

この問題を解決するには,情報統合を視野においた法システムの確立と,併せて,自分のプライバシー情報がどこに存在するのかをデータ主体（個人）が把握し得る個人データ流通管理システム/データ監察官の設置が必要である.

以下,第 2 章では,プライバシー保護制度の流れを概観する.第 3 章では,情報統合によるプライバシー侵害の危険を示す.第 4 章では,ドイツの個人データ保護法等が,情報統合の立場から,どのような施策を講じているかを紹介する.そして,第 5 章では,法システムが具備すべき要件を論じるとともに,個人データ流通管理システム構成を提案する.第 6 章は,まとめである.

2 プライバシーの概念と保護

2.1 プライバシー保護制度の歴史 [1, 2]

1890 年にウォーレンとブランダイスは,プライバシー権を「ひとりで放っておいてもらう権利」と定義した.しかし,1960 年代中頃からのコンピュータの発達により,プライバシー権を従来の受動的権利から,能動的な自己情報がどの様に利用されているかを知る,また間違っていれば訂正できる権利として捉えるべきであることが提唱され,「自己情報コントロール権」としてのプライバシー権が生まれた.

自己情報コントロール権」を保護法益とするプライバシー保護法は,スウェーデン (1973 年),アメリカ (1974) を始めてとして,欧米を中心とした世界各国において制定された.しかし,国外処理規制条項を有するヨーロッパと,情報産業育成を図るアメリカが対立し,その為,OECD（経済開発協力機構 ; Organization for Economic Cooperation and Development）は,1980 年に「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」[9]（以下 OECD 理事会勧告）を採択した.OECD 理事会勧告は,我が国でも,プライバシー保護ガイドラインの基礎となっている.

また,今後の世界的な指針となる EU 指令がある [10].この指令は,「『個人データの処理』を自動的な手段であるかどうかに係わらず個人データに対して行われる作業又は一連の作業を意味するものとする.」（第 2 条 b 項）とするなど,広範囲にわたる個人データの保護を求めている.

2.2 わが国におけるプライバシー保護政策

わが国のプライバシー権は,1959 年の「宴のあと」事件によってその第一歩を示す.東京地方裁判所は,「私生活をみだりに公開されないという法的保障ないし,権利」としてその権利を認めた.しかし,あくまで「ひとりで放っておいてもらう権利」とする伝統的プライバシー権にとどまっていた.しかし,1980 年代に入ると変化がみられる.その原因は OECD 理事会勧告である.種々の議論を経て,1988 年にようやく「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が成立する.この法律が,我が国で唯一の個人データ保護に関する法律である.

2.3 我が国の問題点

我が国の個人データ保護法制は,幾つかの問題を有している.まず,第一に,民間部門に対する規定がなく,地方公共団体にもその適用はなされていない.また,電算化されたデータのみを対象とし,マニュアル処理は含まれない.

民間における個人データの保護については,1987 年に (財) 金融情報システムセンター (FISC) が,

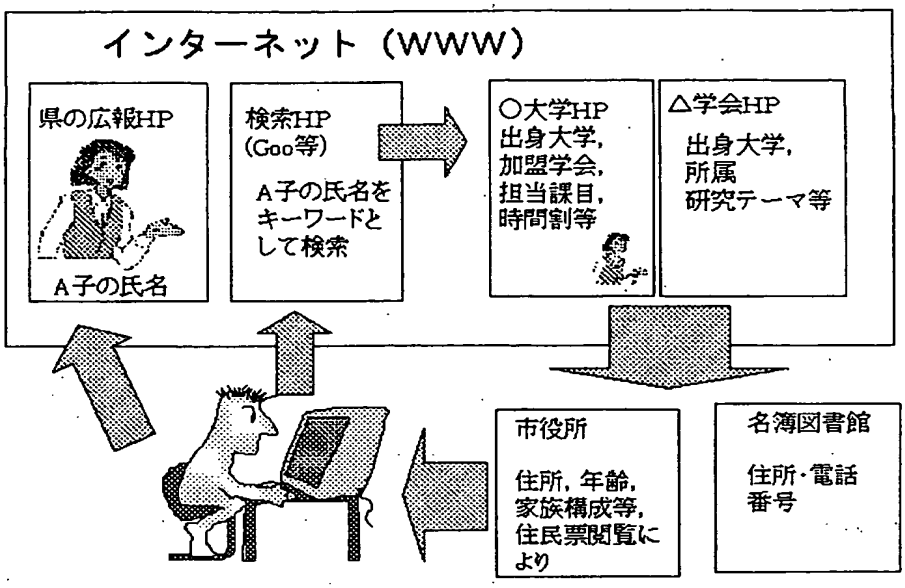

図 1: 情報統合による侵害実行例

「金融機関等における個人情報保護のための取扱指針 [11] を,1989 年には（財）日本情報処理開発協会（JIPDEC）が,「民間部門における個人情報保護のためのガイドライン」[12] を策定,1997 年 1 月に改定を行っている [12]. また、JIPDEC は，我が国における実現可能なプライバシー保護政策の一つとして,「プライバシー保護マーク」を制定しており [13], 同様の試みは、日本データ通信協会 [14] によっても施行されている。日本国内には, 他にも業界毎にガイドラインが存在するが, いずれも法律的な強制力・罰則は有しない [19].

更に, 我が国の法律では, データ管理者の処罰規定はない. 情報化時代においては, データ管理者による犯罪の方が, その損害も深刻なものになる. にもかかわらず, ファイル管理者（及び利用者）に対する罰則が存在しない. また, データ主体の自己情報コントロール権も弱い. 即ち, 権利としての明確な規定はされていない.

また, 諸外国とは異なり, プライバシー侵害への監視機関もない. 諸外国においては, スウェーデンのデータ検査委員, ドイツのデータ保護監督官等のように, 第三者的な監督機関をたてるか, もしくは行政機関の所属であっても独立した権限を与え, その法律の実効性の確保を図っている.

3 インターネットが生む新たなプライバシー侵害

3.1 情報統合の実際

インターネットの広範な普及とともに, ある特定個人の情報が, 断片的に, 複数のホームページ (以下,HP と略記する.) で公開されるようになっている. この様な状況では, 情報を統合することにより発生する新たなプライバシー侵害の可能性がある.

インターネット情報の統合によって起こるプライバシー侵害には, 従来からインターネットにおける問題点として指摘される準拠法と管轄権の問題や, オープンネットワークの特性からの従来のプライバシー保護規制における規制対象となるデータ管理者の不在の問題も含まれる. しかし, 最大の問題は, 各々が合法的な HP を統合的して, プライバシー侵害が行われた場合,HP の責任を問えるのか, という問題である. 以下, 具体的に示す.

前提：女性 A は, 大学の助手であり, 最近, 県 HP に, 受賞者として写真と名前のみが掲載された（自宅住所, 自宅電話番号, 年齢, 生年月日等は掲載せず, プライバシー保護に配慮している）. 但し,A に関する情報は, 所属大学 HP において, 出身大学, 加入学会が掲載されていた.

侵害の実行：県広報 HP の A に興味を持った人物 B が, (Step1) goo 等のサーチエンジンで A の氏名で検索し, (Step2) ヒットした大学や, 学会の HP から,A の出身大学, 所属, 加盟学会等の情報を得る. (Step3) これにより, 県広報に載った女性が (Step2) の助手と分かる. (Step4) 名簿屋に行き大学職員名簿から自宅住所, 電話番号等が判明する. そして市役所で住民票を閲覧すれば, (閲覧規制があれば, 適当な人物に成りすまし, 戸籍や住民票の写しを請求) (Step5) A が一人暮らしであることや, 大学の HP 中に表示されたカリキュラムから自宅にいない時間まで割り出せる.

3.2 数値的評価

日本ユニバックによれば [16], 約 100 の苗字で苗字全体の 37%を占める. 100 万人の被検索対象がある場合に, 上位 100 種の苗字で, 一つの苗字に平均

370,000/100 = 3,700

人がひしめく. 一方, 名前の分布は, 苗字よりも分布が広いと思われるが, 安全側に取って, 苗字と同様とする. この場合, 上位 100 種の名前と苗字の組み合わせで, 特定氏名を持つ同姓同名の人数は,

3,700 × 3,700 /1,000,000 = 13.69

人と少ない. しかし, これでは, 情報統合はできない.

一方, 苗字の 500 位から 1000 位までの人数は, 全体の 10.79%である. この場合, 同一の性を持つ人数は,

0.1079 × 1,000,000 / 500 = 215.8

人にまで減少する. 従って, この 500 位から 1000 位にある範囲にある名前と, ありふれた 100 位までの苗字を組み合わせると, 同姓同名の人数は,

215.8 × 3,700/1,000,000 = 0.798

人となり, 個人を特定できる確率が高い. 実際の名前の分布は, さらに広がりが激しいものと思われ, 被検索人数が 100 万人から増加しても, 苗字又は名前が珍しいなら, 氏名による情報統合が可能と思われる.

では,(Step4) はどの点において問題といえるのか. まず, 名簿屋等の民間業者における個人データの二次利用の問題がある. 名簿情報は, 流通に何ら法的措置は講じられていない. 次に, 未だに戸籍や住民票といった個人データそのものに対してさえ, 制度的なプライバシー保護措置が弱いことも問題であろう.

以上のようにわが国のプライバシー保護制度の未整備は, すでに顕在化している問題とともに, ネットワーク上のプライバシー侵害をもより深刻なものにする. 諸外国並の総合的なプライバシー保護制度の成立が急務である.

3.3 増大する個人データの収集

ネットワーク技術の進展により, 個人データは大規模に蓄積されてゆく. 具体的には, 以下のような技術要素がある.

- **データマイニング技術**： 購買データから, 顧客の購買傾向を発見するデータマイニング技術への期待は極めて大きい. ポイントカード等を利用した, 個人の購買記録の収集は、更に広がる可能性が高い.
- **ロジスティクスの電子帳票 (EDI) 化** 物流の迅速化・効率化の観点から, 搬送される物品種別, 発注者, 送り先等は電子帳票化 (EDI) されて, 細かく管理されている. 最近は, 相乗り形式も多く, 搬送情報は, 多くの企業に流通してゆく.
- **HP 数の増大と XML の登場:** HP の個数が増加するのみでなく,XML[15] によって, データベースがインターネットを流通する. これは, 統合精度を向上させる.
- **企業内ネットワーク化の進展:** 電子メールのログはすべて保存されている. 扶養, 年休等の総務系処理もネットワーク化され, 社員の構内 PHS は、原理的に位置情報がセンターに集約される[1]. また, 社内のセキュリティ管理のため、カードによる認証 (バッチシステム) が行なわれ, 扉の開閉データはすべてセンターに送信・保存される可能性がある. これらはすべて個人データである [20].

このため, 例えば, ネットワークサーバ上のデータを統合して、労組役員や要注意人物の監視, 不倫関係の摘出 (電子メールでの不倫を思わせる連絡を抽出) が可能となる. 総務系システムでは, 同時に年休を取得する妻帯者と若い女性社員のペアを簡単にリストアップできる [20]. しかし, 彼と彼女は, たまたま同時に, ある NGO で奉仕活動をしていただけだったかもしれない.

[1] 今後は, 社内電話がすべてコンピュータテレフォニー化し,LAN ですべての通話が処理される可能性がある. この場合,PBX にくらべてログの取得は容易なはずである.

問題なのは, いわゆる「名簿屋」が, 購買データや, インターネット上のデータ等を販売するようになる可能性があることである. 最初から電子化されたデータは, 買い手にとっても魅力的である. そして, 民間部門に対するプライバシー保護法制のない我が国で, これらの行為をどこまで, 法的に規制し得るかは疑問である.

但し, 本来の目的である EC (電子商取引 : Electronic Commerce) やポイントカード等の, 経済的利点を妨げてはならない. 顧客の購買行動を広く収集できれば, 設計・製造・物流・資源回収のサプライチェーンを効率化・迅速化できる可能性がある. そして, このような SCM(Supply Chain Management) により, 企業の競争力を強化し, 併せて限りある資源の有効利用を図る事は, 経済活性化のためにも, 「環境にやさしい持続できる経済的発展」にも重要である.

藤原は, プライバシー法と環境法の類似を指摘している [3]. 上記のような, 多様なサービスが実現されるなかで, 各々のサービスの利点を生かしながら, 一方, プライバシーを保護し, しかも必要な官庁等の情報公開を進める必要がある. どれをどう情報統合すると, プライバシーが漏洩するかの分析は容易ではない. これらを総合的に満足する個人データ流通と保護のあり方は現在未だ得られていない.

4 諸外国の法制度

4.1 EU 指令

海外には, 不十分ながらも, 情報統合への配慮を行っている法制が存在する.1995 年ヨーロッパ連合 (EU) は,1998 年 10 月までの域内各国の法的対応を義務づけた, プライバシー保護のための指令「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」[10] を出した.EU 指令は, 今後の世界各国のプライバシー保護政策の指針となるものと考えられ, 以下の通り, 情報統合に関係した記述がある.

「個人データの処理」(処理) とは, 自動的な手段であるかどうかに関わらず, 個人データに対して ‥ (中略) ‥ 開示, もしくは連結, ブロック化, 消去又は破壊が含まれる.

上記連結 (combination) のなかに, 情報統合を含めるのが自然であろう. 一方, 最も進んだ法制度を有するのは, ドイツである. 情報統合を意識した条文が存在する. 次にドイツ法について紹介する.

4.2 ドイツにおける個人データ保護法制

4.2.1 ドイツの ID カード [6]

ドイツでは, 住民の氏名, 住所等の情報を記録した ID カードの携帯が義務づけられている.ID カードには, 各行政機関が住民に対してなした行政サービスの履歴を記録できる仕様のものがあり, これと国民背番号制が結合され, インターネットによる情報統合が絡めば, 個人データは丸裸同然となる.

しかし,1986 年の身分証明書法の中で,ID カード記載事項は, 専ら ID カードを作成以外の目的では利用してはならず, 使用後ただちに消去しなければならない (第 3 条第 3 項). 一連番号は, 電子計算機ファイルから個人データを呼び出したり, データベースを結合するために利用してはならない (第 4 条第 1 項). と規定している. キー属性である ID カード番号の利用に歯止めをかけている.

また,ID カードの有効期限は 10 年 (26 歳未満は 5 年) として, 更新時には, 別番号を振って, 個人識別に利用できないように配慮している点からも, 立法時の配慮が感じられる. しかし, この法律は, あくまで ID カードに関するものであり, より, 一般的なプライバシー保護は, 次のテレサービスデータ保護法に見られる.

4.2.2 テレサービスデータ保護法

1997 年に制定されたこの法律は, テレサービスで流通する個人データが加工, 利用される際, データ主体がそのことを把握できない状況に鑑み, 従来の個人データ保護法規を補完するために, 制定されたものであり, 「ユーザー・プロフィールの形成・開示の回避」を狙いとする. 取得された情報の分散保存を要求することで, ネットワーク上での情報統合によるユーザー・プロフィールの醸成に歯止めをかけようとの主旨である. 本法のテレサービス提供者を対象とした規定の適用に, 業務性の有無は関係しない. テレサービス提供者は, サービス提供に用いる技術においても, 最低限 の個人データで稼働するようシステムを構成する「省個人データ型システム」への転換を要求しているなど, 興味深い. 詳細は文献 [4, 5] に譲るが, 情報統合に関して特徴的なのは, 以下の部分である.

- **テレサービス利用データの抹消義務:** ユーザーのテレサービスへの接続その他利用について提供者が取得 した情報は, 利用料金請求のために必要とされない限り, 当該ユーザーの利用終了後, ただちに抹消されねばならない. そして, 同一ユーザーによる多種のサービス利用に関して生じた個人データは, 利用料金請求目的以外に統合できない.

- **仮名よる利用履歴の蓄積:** 利用履歴の作成は, 仮名でのみ可能. 当該利用履歴と仮名と本名の情報 を同一に保存する事はできない. これは, 誰のものかを抹消して, データを流通させようとするものである.

5 情報統合への対策

5.1 現行法制の分析

以上紹介したドイツ法の制定によっても, なお, 準拠法の問題等を解決するための手段は提起されていない. しかし, マルチメディア法は, 情報通信における企業活動促進のための出発点となる枠組みを提供した点で評価しうる. 特に, 個人と特定できる情報の消去を迫るドイツ法は, 民間部門に対するプライバシー保護法制を持たない我が国にとっては「雲の上」である.

しかし, 情報技術的に考えると, 多少の疑問を感じざるを得ない. 以下に列挙する.

- **データ主体のプライバシー情報確認のための具体的手段の不明確さ:** ドイツマルチメディア法は, データ主体のプライバシー情報提供了承においても, マウスクリックの利用を忌避するなど, 厳密であるしかし, 具体的に, どこにどんなデータが存在するかを報知するシステムの構成については未検討である.

- **キー属性による結合 (JOIN) のみを想定して良いか?:** どの法制度でも, 結合は, その属性値により一意に個人を特定できるキー属性を前提として考察している. しかし, 氏名などという, 非キー属性であっても, 高い確率で, 情報を統合できる. さらに複数属性の併用が効果的である.

  たとえば,7 桁郵便番号と氏名を利用すると, 対象となる母集団が, 前述の 100 万人ではなく,1 万人程度に低下する. 抽出される人数の期待値は, 上位 100 種の苗字でも, 単一の苗字に僅か

  $3{,}700/100 = 37$

  人となり, 上位 100 種の名前と苗字の組み合わせでも,

  $37 \times 37/10000 = 0.1369$

  人しかいない. つまり, 複数属性を利用すると,ID 番号なしに個人特定が可能と思われる. しかし, このような手法への配慮は, 現行法制には見られない.

更に, 日本では, 業界団体ごとに独自の管理機関が存在し, 個人の信用情報は, 銀行→サラ金と言うように, 業種を越えて交換される. しかし, 登録された信用情報のその後の流通 について, 利用者は, 知る術もほとんど無い.

少なくとも社会制度の面からは, (1) 情報統合そのものを禁止する事, (2) 利用者が自己に関する情報を検索しやすくなる (個人データに関する相談コーナー設置, ドイツの法制にあるデータ保護観察官制度の導入, サ ーバー会社の公的機関への登録義務とレイティング等) 制度を考える必要がある.

5.2 個人データ流通管理システムの提案

情報統合によるプライバシー侵害を防ぐには, データ主体が, 自己のデータの所在場所を知ることが重要である. 所在が分かれば, 開示請求でき, 如何なる情報統合が可能であるかも判定できる. そこで, 本節では, データ主体が認証したデータ管理者以外にはデータが流通せず, かつ, 自分のデータがどこに存在するかを確実に認識できるシステムの一構成法を提案する.

5.2.1 前提条件

個人データ流通管理システム構成の検討の前提として, 以下の条件を設定する.

【要件 1】データ主体による認証:
個人データは, データ主体の承認が無い限り, 記憶してはならない. 但し, 個人データは, つぎつぎと転記される場合もあると思われるので, その場合には, 転記元の認証で良いとする.

【要件 2】データ存在場所の確認:
データ主体は, いつでも, 自分のデータがどこにあるかを確認できなければならない. この実現手段として, 本システムでは, 個人データを保持するデータ管

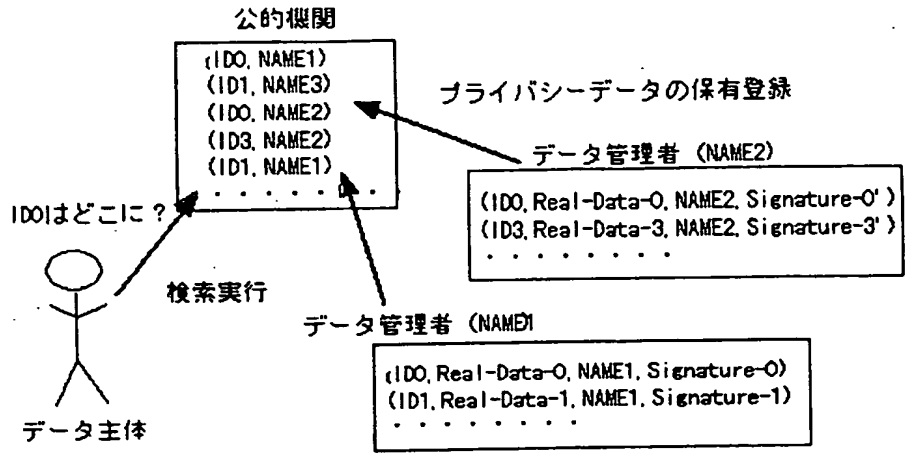

図 2: 個人データ流通管理システム

理者は, データ保持している事を, 公的機関に開示する必要がある.

【要件 3】データ具体値の守秘：
上記公的機関は, 誰のデータがデータ管理者により保持されているのか, それが, いかなるデータ値であるかを登録されたデータから解析できない必要がある.

上記 3 要件を満たすシステムの一例として, 以下の構成を提案する (図 2 参照).

【個人データの保存方法】
個人データは,

ID_i:データ主体 i が作成した秘密の ID 番号
D_p:個人データ
MD:データ管理者名 (企業等の名称)
$S(d)$:データ d へのデータ主体 i のデジタル署名[2]

で表す時,

$ID_i, D_p, MD, S(ID_i + D_p + MD)$

として, データ管理者において保存されるものとする. 但し,$S(ID_i + D_p + MD)$ は,ID_i ,D_p及び MD 全体に対するデータ主体によるデジタル署名 [18] である. これにより, データ主体の了承のもとに, 個人データがデータ管理者に渡されていることが認証される. データ主体の識別番号 は, 極めて大きな桁数の整数からランダムに選択する. これにより,ID 番号の衝突の危険は, 限りなくゼロに近づくことになる. 尚, ここでは省略しているが, データと共に, データ主体の公開鍵の CA 証明書を添付する.

データ管理者は, あらかじめデータ主体との契約により, 他データ管理者に写しを渡すこともある. 写しを作成するたびに, データ主体の署名を受けるのは実際的ではないので, データ管理者が他のデータ管理者にデータを転送する時には, 自分で認証をする. 即ち, この場合の受け取り側が管理するデータは,

$ID_i, D_p, MD', S'(ID_i + D_p + MD')$

となる. 但し, ここで,MD'は受け取り側のデータ管理者名であり,$S'(ID_i + D_p + MD')$ は, コピー元データ管理者によるデジタル認証を意味する. 添付される CA 証明書は, コピー元データ管理者の公開鍵に対する証明書である. 以上のデータ形式以外の個人データ保存を認めないこととすれば, 認証できるのはデータ主体のみであるから, データ管理者が勝手にデータを作成することは出来ない.

【公的機関への個人データ存在の登録】
データ管理者は公的機関に個人データを登録しなければ違法とする. 但し, 実データを登録すると公的機関にプライバシー漏洩するので, データ主体の識別番号である ID_iをデータ管理者識別名称とともにペアとして登録する ((ID_i, MD) あるいは (ID_i, MD') である). 尚, 何個のデータを保持しているかはデータ管理者の法人プライバシーであるとも考えられ, データ管理者は適当に生成した ID による偽データを登録してもよい.

データ主体は, 自己の ID 番号で, 公的機関のデータを検索する. ただし, この際, データ主体は, 自分

[2]個人のデジタル署名を付すことは, 結果として, 不正に当該データが流出したときに, それを否認できない. この問題を解決するには, 認証に, かならず個人に戻る必要がある否認不可署名 [18] の利用が効果的である. 以下の議論は, 否認不可署名であると考えても, 同様である.

のID番号で直接検索することはしない．例えば,IDのビット列の部分値を検索条件として,極めて冗長なデータを取得し,真のIDにより選択する．この際,偽の部分値を入力してもよい．

以上の対策により,公的機関は,データ主体の真のIDが何なのか,即ち,どこにデータ主体の個人データがあるのかを知ることはできない．そして,データ主体は,データ管理者に開示請求をして,その具体値を確認できる．尚,ここで論じたのはデータのありかを確認するシステムであり,言うまでもなく,どのデータをだれが参照しているかを登録・表示するホームページも必要であることは言うまでもない．データベースとして保有していなくても,参照可能であれば,その参照値を統合に利用できるからである．

6 終わりに

情報統合によるプライバシー侵害について紹介し,特に,ヨーロッパ法で想定している個人IDによる結合ではなく,複数属性による統合の危険の問題を提起した．今後の法システム設計にあたっては,情報統合への配慮が必要であり,欧米のデータ監察官を我が国に導入する場合でも,配慮が必要と考える．

情報統合の危険を予知するには,(1) 個人データの所在をデータ主体が知り得るシステム,(2) 個人データが誰から見えているかを知り得るシステムが必要である．その実現法のひとつとして,本論文では,デジタル署名による個人データ流通管理システムを提案した．

一方,ネットワーク化により,電子商取引(EC),ポイントカード等による顧客データの蓄積等,個人データを収集するシステムは膨張を続けている．これらは,我が国経済の発展のためにも普及させるべき技術である．しかし,民間部門へのプライバシー保護法制を持たない我が国では,このデータが「名簿屋」に流れない保障はない．最初から電子化された顧客データは,名簿屋にとっても,買い手にとっても,魅力的な商品である．

顧客データ利用等による経済活性化,官庁等の情報公開,そしてプライバシー保護．これらは,いずれも発展させねばならず,相互に関連が深い．しかし,健全なネットワーク経済の発展と,個人の尊重を同時に実現できる,総合的な法とシステムの形態は未だ見えない．にも関わらず,ネットワーク化は急速である．総合的な対策のために残された時間は少ない．そのことが,今回の報告をまとめるにあたり,最も強く残った印象である．

参考文献

[1] 堀部政男,「プライバシーと高度情報化社会」,岩波書店,1988.

[2] 堀部政男(編),「情報公開・プライバシーの比較法」,日本評論社,1996.

[3] 藤原静雄,「個人データの保護」,岩波講座現代の法(10)情報と法,岩波書店,1997.

[4] 米丸恒治,「ドイツ流サイバースペース規制」,立命館法学,No.255,pp.141–194,1997.

[5] 小澤哲郎,「ドイツマルチメディア法〜情報及び通信サービスの枠組みを定める法律〜」,国際商事法務,Vol.26,No.3,pp.277–287,1998.

[6] 平松毅,「情報公開と個人情報保護」,公法研究,NO.60,pp.1–24,1998.

[7] 本村憲史,金田重郎,「ネットワーク上での情報統合によるプライバシー侵害とその対策」,電子情報通信学会技術研究報告 OFS98–5,pp.29–36,1998.

[8] 本村憲史,金田重郎,「ネットワーク上での情報統合によるプライバシー侵害とその対策」,経営情報学会 1998 年春季全国研究発表大会,D–1–2,pp.65–68,1998.

[9] OECD ガイドライン,"1980 Organization for Economic Cooperation and Development Guidelines on Privacy and Transborder flows", http://www.oecd.org/dsti/iccp/legal/priv-en.html, 1980,(邦訳は,ECOM の HP,http://www.ecom.or.jp/)

[10] EU 指令,"Directive 95. EC of the European Parliament and of the Council of On the protection of individuals with regard to the processing of personal data and on the free movement of such data", 1995,(邦訳は,ECOM の HP,http://www.ecom.or.jp/).

[11] 財団法人・金融情報システムセンター編,金融機関等における個人データ保護,金融情報システムセンター発行,1991(但し,FISC はガイドラインの改定を進めている).

[12] 日本情報処理開発協会(JIPDEC)ガイドライン (http://www.jipdec.or.jp/security/privacy.htm).

[13] プライバシーマーク制度(JIPDEC) http://www.jipdec.or.jp/security/MarkSystem.html/.

[14] (財)日本データ通信協会プライバシーマーク制度の創設・運用開始について http://www.dekyo.or.jp/hogo/center.htm/.

[15] 村田真,「XML 入門」,日本経済新聞社,1998.

[16] 丹羽基二(監),日本ユニバック(編),「日本の苗字」,日本経済新聞社,1971.

[17] 岡本龍明,山本博資,「現代暗号」,産業図書,1997.

[18] D.R.Stinson 著,櫻井幸一監訳,「暗号理論の基礎」,共立出版社,1996.

[19] 社団法人・情報サービス産業協会(JISA)のリンク集に国内のリンクがよくまとめられている.http://www.jisa.or.jp/privacy/link-j.html/.

[20] 企業内部の個人情報の扱いについての個人情報に関する関心も薄いと言われる．例えば労働省の報告を参照.http://www.jil.go.jp/kisya/daijin/980629_01_d/980629_01_d.html/.

複写される方に

情報処理学会研究報告
IPSJ SIG Notes
情処研報 Vol.99, No.11
1999年1月30日発行

発行所 〒108-0023 東京都港区芝浦三丁目 16 番 20 号
芝浦前川ビル 7 階

社団法人 情 報 処 理 学 会 TEL 東京(03)5484-3535 (代表)
郵便振替口座 (00150-4-83484)

発行人 社団法人 情 報 処 理 学 会 柳 川 隆 之
Information Processing Society of Japan